IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

QOTD FILM INVESTMENT LTD A United Kingdom Limited Company Plaintiff, v. **DOES 1-26**, Defendants.	)	Case No.: 2:16-cv-11275 Hon. Judge Matthew F. Leitman Magistrate Judge Stephanie Dawkins Davis

AMENDED MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(f) CONFERENCE

Pursuant to Fed. R. Civ. P. 26(d)(1), and upon the attached: (1) Memorandum of Law in support of this motion; and (2) Declaration of David Macek submitted in support of this motion, Plaintiff respectfully moves for entry of an order granting leave to serve third party subpoenas upon the Internet Service Providers identified in Exhibit 1 prior to a Rule 26(f) conference (the "Motion"). A proposed order is attached for the Court's convenience.

Oral hearing requested.

DATED: April 8, 2016

Respectfully submitted,

By: s/Barry C. Kane
Barry C. Kane (P-45851)
KANE & CO., PLC
29 Pearl St. N.W.
410 Federal Square Building
Grand Rapids, MI 49503
(616)726-5905 (v)
(616)726-5906 (f)
e-mail:bkane@kaneplc.com
http://www.kaneplc.com

ATTORNEY FOR PLAINTIFF

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

QOTD FILM INVESTMENT LTD A United Kingdom Limited Company Plaintiff, v. **DOES 1-26**, Defendants.	)	Case No.: 2:16-cv-11275 Hon. Judge Matthew F. Leitman Magistrate Judge Stephanie Dawkins Davis

MEMORANDUM IN SUPPORT OF PLAINTIFF'S AMENDED MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE
ORAL HEARING REQUESTED

I. Introduction

This action seeks to address the infringement of Plaintiff's copyrighted motion picture entitled "*Queen of the Desert*" (the "Film"). The alleged Defendants are only known at this time by their Internet Protocol (IP) address. Plaintiff must take early discovery of the Internet Service Providers of the Defendants to obtain their true names, addresses, and account information.

The Film is a chronical of Gertrude Bell's life, a traveler, writer, archeologist, explorer, cartographer, and political attaché for the British Empire at the dawn of the twentieth century. The critically acclaimed film was written and directed by Werner Herzog and starts James Franco, Nicole Kidman, Robert Pattinson among others. This film has been estimated to have been illegally copied by thousands since its release.

A. Peer-to-Peer File Sharing

Illegally downloading mainstream movies to avoid purchasing a ticket, the DVD or a rental fee is so pervasive that the public widely accepts it without question. There are even

websites devoted to illegal copying. One such website is *The Pirate Bay* where instructions on how to download the required pirating software, usually a torrent, may be obtained.1 *The Pirate Bay* website even provides a convenient "Pirate Search" tab that enables copiers to "shop" for illegal copies of games, music, movies, books and software. This illegal copying clearly is an intentional act since it requires an infringer to install special software and search out movies to pirate. This is the problem this action seeks to address.

Cloaked in the anonymity of the Internet, digital pirates band together into swarms using file-sharing technology such as BitTorrent to illegally obtain and distribute high quality copies of the Film. While each single act of infringement may appear to be slight, collectively, illegal downloading often starts even before a movie is released and costs legitimate industries millions of dollars. Exhibit A. Not only are movies pilfered, the pirates" other prizes include TV shows, computer games, e-books, software and music.

This suit not only represents a single copyright owner faced with the daunting task of protecting its Intellectual Property from the irreparable harm caused by over one-hundred-thousand swarming infringers, it is emblematic of the fight of the motion picture industry and any other legitimate businesses that rely on copyright protection. Denying Plaintiff the discovery needed to pursue the infringing swarm in a single action endorses and encourages the infringement. It frees the pirates to roam the Internet searching for prizes by providing shelter through the anonymity of the Internet and the high cost of individual enforcement.

B. Who Are the "Does"

Plaintiff has named the Defendants as "Does" because they committed the infringement using pseudonyms ("user names" or "network names"), not their true names. Plaintiff has only been able to identify the Doe Defendants by (1) their Internet Protocol ("IP") addresses, (2) the dates and times of the infringement, (3) the file hash value which identifies each Defendant as cooperatively participating in the same swarm and (4) the location of each IP address.

Defendants' actual names may only be obtained from the non-party Internet Service Providers ("ISPs") to which the Defendants subscribe and from which the Defendants obtain

Internet access, as this information is readily available to the ISPs from documents kept in the regular course of business. Accordingly, Plaintiff seeks the leave of the Court to serve limited discovery prior to the Rule 26(f) conference on the non-party ISPs solely to determine the true identities of the Doe Defendants. Plaintiff requests that the Court allow Plaintiff to serve Rule 45 subpoenas on the ISPs immediately so as not to delay this case, and to allow the ISPs the time necessary to comply with the safe-harbor provisions of giving notice to their subscribers.

Should the Court grant this Motion, Plaintiff will serve subpoenas on the ISPs requesting them to produce the identifying information. The ISPs will be able to notify their subscribers that this information is being sought, and, if so notified, each Defendant will have the opportunity to raise any objections before this Court. Thus, to the extent that any Defendant wishes to object, he or she will be able to do so.

II. Argument

Pursuant to Rule 26(d)(1), except for circumstances not applicable here, absent a court order, a party may not propound discovery in advance of a Rule 26(f) conference. Rule 26(b) provides courts with the authority to issue such an order: "[f]or good cause, the court may order discovery of any matter relevant to the subject matter involved in the action." *Turner Industries Group, LLC vs. International Union of Operating Engineers, Local 450,* U.S. Dist. LEXIS 68746, at *7-*10 (S. D. Tex. 2013). In Internet infringement cases, courts routinely find good cause exists to issue a Rule 45 subpoena to discover a Doe defendant's identity, prior to a Rule 26(f) conference, where: (1) the plaintiff makes a prima facie showing of a claim of copyright infringement, (2) plaintiff submits a specific discovery request, (3) there is an absence of alternative means to obtain the subpoenaed information, (4) there is a central need for the subpoenaed information, and (5) defendants have a minimal expectation of privacy. *See Arista Records, LLC v. Doe 3,* 604 F.3d 110 (2d Cir. 2010) (citing *Sony Music Entm't v. Does 1-40*, 326 F.Supp.2d 556, 564-65 (S.D.N.Y. 2004) (numbers added)); *Elektra Entm't Group, Inc. v. Doe*, No. 5:08-CV-115-FL, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008) (same); *Warner Bros. Records, Inc. v. Doe*, No. 5:08-CV-116-FL, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008)

(same); *BMG Music v. Doe # 4*, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (same). *See also, Arista Records LLC v. Does 1-19*, 551 F.Supp.2d 1, 6-7 (D.D.C. 2008), and the cases cited therein, noting the "overwhelming" number of cases where copyright infringement plaintiffs sought to identify "Doe" defendants and courts "routinely applied" the good cause standard to permit discovery. Here, all of the good cause elements are present. Thus, this Court should grant the Motion.

A. Precedent Allowing Discovery to Identify Doe Defendants

In copyright cases brought by motion picture studios and record companies against Doe defendants, this Court and other courts have granted leave to take expedited discovery to serve subpoenas on ISPs to obtain the identities of Doe Defendants prior to a Rule 26 conference. *TCYK, LLC v Does 1-9*, 13-cv-14322 (E.D. Mich. December 2, 2013)(Doc. 9); *Patrick Collins Inc. v John Does 1-21*, 282 F.R.D. 161, 2012 WL 1198040 (E.D. Mich. 2012); *Warner Bros. Records, Inc. v. Does 1-6*, 527 F.Supp.2d 1, 2 (D.D.C. 2007) (allowing plaintiffs to serve a Rule 45 subpoena upon Georgetown University to obtain the true identity of each Doe defendant, including each defendant's true name, current and permanent addresses and telephone numbers, email address, and Media Access Control ("MAC") address) (citing Memorandum Opinion and Order, *UMG Recordings, Inc. v. Does 1-199*, No. 04-093(CKK) (D.D.C. March 10, 2004); Order, *UMG Recordings v. Does 1-4*, 64 Fed. R. Serv. 3d (Callaghan) 305 (N.D. Cal. March 6, 2006)).

The following factors are considered when granting motions for expedited discovery to identify anonymous Internet users: (1) whether the plaintiff can identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court; (2) all previous steps taken by the plaintiff to identify the Doe Defendant have been unsuccessful; and (3) whether the plaintiff's suit could withstand a motion to dismiss. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999).

B. Good Cause Exists to Grant the Motion

1. Plaintiff's Prima Facie Claim for Copyright Infringement

a. Overview of Allegations and Factual Showings

The Complaint alleges that the Doe Defendants, without authorization, used an online media distribution system to cooperatively download the copyrighted Film and to cooperatively distribute it to other users on the P2P network, including by making the copyrighted Film for which Plaintiff holds the exclusive reproduction and distribution rights. (Compl. ¶¶ 11-18) Maverickeye UG ("MEU"), a provider of online anti-piracy services for the film industry, was engaged to monitor this infringing activity. Exhibit A; Declaration of Daniel Macek ("Macek Decl.").

An IP address is a unique numerical identifier that is automatically assigned to an Internet user by the user's Internet Service Provider ("ISP"). In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the user/subscriber. (Macek Decl., ¶ 17).

Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of Internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used. Unfortunately, many ISPs only retain for a very limited amount of time the information necessary to correlate an IP address to a particular subscriber. (Macek Decl., ¶18).

To identify the IP addresses of those torrent users who were copying and distributing Plaintiff's copyrighted Film, Daniel Macek, a software consultant with MEU, was responsible for analyzing, reviewing and attesting to the results of the investigation. (Macek Decl., ¶¶ 19-22).

Forensic software provided by MEU to scan peer-to-peer networks for the presence of infringing transactions (Macek Decl., ¶23) and the IP addresses of the users responsible for copying and distributing the Film were isolated. (Macek Decl., ¶24) Through each of the

transactions, the computers using the IP addresses identified in Complaint Exhibit 1 transmitted a copy or a part of a copy of a digital media file identified by the relevant hash value. The IP addresses, hash values, dates and times contained in Complaint Exhibit 1 correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in Complaint Exhibit 1 were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted work. (Macek Decl., ¶25)

Moreover, the users were sharing the exact same copy of the Film. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum," also referred to as a hash file. The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1", which was developed by the National Security Agency and published as a US government standard. Using a hash checksum to identify different copies of the Film, it was confirmed that these users reproduced the very same copy of the Film. (Macek Decl., ¶26)

The MEU software analyzed each Torrent "piece" distributed by each IP address listed in Complaint Exhibit 1 and verified that reassembling the pieces using a specialized Torrent client results in a fully playable digital copy of the Film. (Macek Decl., ¶27).

The software uses a geolocation functionality to confirm that all IP addresses of the users set forth in Complaint Exhibit 1 are accurate. Though an IP address alone does not reveal the name or contact information of the account holder, it does reveal the locations of the Internet line used for the transaction. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. In the United States, these blocks are assigned and tracked by the American Registry of Internet Numbers. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP addresses geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs. (Macek Decl., ¶28).

b. Plaintiff's Prima Facie Showing of Copyright Infringement

Plaintiff has sufficiently identified the Doe Defendants through the unique IP address that each Doe Defendant was assigned at the time of the unauthorized distribution and copying of the copyrighted Film. These Defendants gained access to the Internet through their respective ISPs by setting up an account with the various ISPs. The ISPs can identify each Defendant by name through the IP address by reviewing its subscriber activity logs. Thus, Plaintiff can show that all Defendants are "real persons" whose names are known to the ISP and who can be sued in federal court.

A prima facie claim of copyright infringement consists of two elements: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340, 361 (1991). Plaintiff satisfied the first good cause factor by properly pleading a cause of action for copyright infringement. (Compl. at ¶¶ 11-18) *In re Aimster Copyright Litig.*, 334 F.3d 643, 645 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004) ("Teenagers and young adults who have access to the Internet like to swap computer files containing popular music. If the music is copyrighted, such swapping, which involves making and transmitting a digital copy of the music, infringes copyright."); *Elektra Entm't Group, Inc. v. Doe*, No. 5:08-CV-115-FL, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008) ("[P]laintiffs have established a prima facie claim for copyright infringement, as they have sufficiently alleged both ownership of a valid copyright and encroachment upon at least one of the exclusive rights afforded by the copyright."); *Warner Bros. Records, Inc. v. Doe*, No. 5:08-CV-116-FL, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008) (same). Accordingly, Plaintiff has exceeded its obligation to plead a prima facie case.

2. Plaintiff Seeks Limited and Specific Discovery

Plaintiff only seeks to discover the name and address of the Defendants. This is all specific information that is in the possession of the Defendant's ISP that will enable Plaintiff to

advance the action. Since the requested discovery is limited and specific, Plaintiff has satisfied the second good cause factor.

3. No Alternative Means Exist to Obtain Defendant's True Identities

Other than receiving the information from the Defendants' ISP, there is no way to obtain Defendants' true identity because the ISP is the only party who possesses records which track IP address assignment to their subscribers. Consequently, the ISP is the source for information relating to associating an IP address to a real person. Since there is no other way for Plaintiff to obtain Defendant's identity, except by serving a subpoena on Defendant's ISPs demanding it, Plaintiff has established the third good cause factor. *See Columbia Ins. Co. v. Sees Candy et al.*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999); *Elektra Entm't Group, Inc. v. Doe*, No. 5:08-CV-115-FL, 2008 WL 5111886, at *4 (E.D.N.C. Dec. 4, 2008) (finding that the feasibility of a suggested alternative method of determining defendants‟ identities by hiring a private investigator to observe downloading "is questionable at best"); *Warner Bros. Records, Inc. v. Doe*, No. 5:08-CV-116-FL, 2008 WL 5111883, at *4 (E.D.N.C. Dec 4, 2008) (same).

4. Discovery Is Needed to Advance the Asserted Claims

Plaintiff will not be able to serve the Defendants with process and proceed with this case without the requested discovery. Plaintiff's statutorily protected property rights are at issue in this suit and, therefore, the equities should weigh heavily in favor of preserving Plaintiff's rights. Since identifying the Defendant by name is necessary for Plaintiff to advance the asserted claims, Plaintiff has established the fourth good cause factor. *Sony*, 326 F.Supp. at 566; *BMG Music v. Doe # 4*, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (finding under nearly identical circumstances that "[p]laintiffs have shown that the subpoenaed information—Doe # 4‟s identity—is centrally needed to advance Plaintiffs‟ copyright infringement claim").

5. Plaintiff's Interest in Knowing Defendant's True Identities Outweighs Defendant's Interests in Remaining Anonymous

Plaintiff has a strong legitimate interest in protecting its copyright. Defendants are copyright infringers with no legitimate expectation of privacy in the subscriber information provided to the ISP, much less in distributing the copyrighted work in question without permission. *See Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); *BMG Music v. Doe # 4*, No. 1:08-CV-135, 2009 WL 2244108, at *3 (M.D.N.C. July 24, 2009) (finding under nearly identical circumstances that "[p]laintiffs have shown that Defendant Doe # 4 has a minimal expectation of privacy downloading and distributing copyrighted songs without permission"); *Interscope Records v. Does 1-14*, 558 F.Supp.2d 1176, 1178 (D. Kan. 2008) (a person using the Internet to distribute or download copyrighted music without authorization is not entitled to have their identity protected from disclosure under the First Amendment); *Sony*, 326 F.Supp.2d at 566 ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission"); *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 8-9 (D.D.C. Apr. 28, 2008) (finding that the "speech" at issue was that doe defendant's alleged infringement of copyrights and that "courts have routinely held that a defendant's First Amendment privacy interests are exceedingly small where the …speech "is the alleged infringement of copyrights"); *Sony Music Entm't, Inc. v. Does 1–40*, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004) ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission"); *Arista Records, LLC v. Doe No. 1*, 254 F.R.D. 480, 481 (E.D.N.C. 2008); *U.S. v. Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000).

Downloading a mainstream motion picture is no different than downloading a song. Being named as a defendant in this action does not expose an individual to embarrassment. It is not blackmail. In fact, copying music and mainstream movies is so pervasive that the public widely accepts it without question. And, this is the exact problem this lawsuit addresses. That copying a mainstream movie is no different than downloading a song, it raises no privacy concerns.

C. Irreparable Harm Establishes Good Cause to Grant the Motion

Good cause exists here for the additional reason that a claim for copyright infringement presumes irreparable harm to the copyright owner. This is especially true in this matter since the copying results in financial losses such as lost ticket sales and eroding rentals and purchases. *See UMG Recordings, Inc. v. Doe*, 2008 WL 4104214 (N.D. Cal. 2008) (finding good cause for expedited discovery exists in Internet infringement cases, where a plaintiff makes a prima facie showing of infringement, there is no other way to identify the Doe defendant, and there is a risk an ISP will destroy its logs prior to the conference); Melville B. Nimmer & David Nimmer, *Nimmer on Copyright*, § 14.06[A], at 14-03 (2003); *Elvis Presley Enter., Inc. v. Passport Video*, 349 F.3d 622, 631 (9th Cir. 2003).

The first and necessary step that Plaintiff must take to stop the infringement of its valuable copyright is to identify the Doe Defendants who are copying and distributing the Film. This lawsuit cannot proceed without the limited discovery Plaintiff seeks because the ISPs are the only entities that can identify the otherwise anonymous Defendants. Courts regularly permit early discovery where such discovery will "substantially contribute to moving th[e] case forward." *Semitool*, 208 F.R.D. at 277.

III. Conclusion

For the foregoing reasons, Plaintiff respectfully submits that the Court should grant the pending Motion for Leave to Take Discovery Prior to the Rule 26 Conference. Plaintiff requests permission to serve a Rule 45 subpoena on the ISPs it has identified as of this date, and those it identifies in the future, so that the ISPs can divulge the true name and address of each Doe Defendant that Plaintiff has identified to date, and those it identifies in the future during the course of this litigation and an order that the ISPs shall comply with the subpoenas. Plaintiff will only use this information to prosecute its claims. Without this information, Plaintiff cannot pursue its lawsuit to protect its Film from past and ongoing, repeated infringement.

DATED: April 8, 2016 Respectfully submitted,

By: s/Barry C. Kane
Barry C. Kane (P-45851)
KANE & CO., PLC
29 Pearl St. N.W.
410 Federal Square Building
Grand Rapids, MI 49503
(616) 726-5905 (v)
(616) 726-5906 (f)
e-mail: bkane@kaneplc.com
Web: kaneplc.com

ATTORNEY FOR PLAINTIFF

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

QOTD FILM INVESTMENT LTD A United Kingdom Limited Company Plaintiff, v. **DOES 1-26**, Defendants.	)	Case No.: 2:16-cv-11275 Hon. Judge Magistrate Judge

DECLARATION OF DANIEL MACEK IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

1. My name is Daniel Macek. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

2. I am an employee at Maverickeye UG ("MEU"), a company incorporated in Stuttgart and organized and existing under the laws of Germany, in its technical department. MEU is in the business of providing forensic investigation services to copyright owners.

3. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows users to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data.

4. The Internet also affords opportunities for the wide-scale infringement of copyrighted motion pictures and other digital content.

5. Once a motion picture has been transformed into a digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

6. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called peer-to peer ("P2P") or BitTorrent networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

7. To use a P2P or BitTorrent distribution system requires more than a click of a button. A software installation and configuration process needs to take place.

8. The P2P systems enable widespread distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to other users and so on, so that complete digital copies can be easily and quickly distributed thereby eliminating long download times.

9. While Plaintiff has observed the infringement occurring on the Internet, it does not know the true identities of those individuals who are committing the infringement.

10. Additionally, the P2P methodologies for which Maverickeye UG monitored for Plaintiff's Motion Picture make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users ("peers") on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from where the file can be

downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together to comprise the whole.

11. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network can also be a source of download for that infringing file, potentially both copying and distributing the infringing Motion Picture. The distributed nature of P2P leads to rapid spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent.

12. All infringers connected to those files are investigated through downloading a part of the file placed on their computer.

13. This evidence including the date it was first downloaded is then saved on a secure server.

14. Once the searching software program identifies an infringer in the way described herein for the Motion Picture for which Plaintiff owns the exclusive licensing and distribution rights, it automatically obtains the IP address of a user offering the file for download and saves it in a secure database.

15. The forensic software routinely collects, identifies and records the Internet Protocol ("IP") addresses in use by those people who employ the BitTorrent protocol to share, copy, reproduce and distribute copyrighted works. In this way the software is connected to files of illegal versions of the Motion Picture.

16. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP"). It only enables Plaintiff to trace the infringer's access to the Internet to a particular ISP. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority ("IANA") or a regional internet registry such as the American Registry for Internet Numbers ("ARIN"). However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. These intermediaries can be identified by the ISP and the intermediaries own logs will contain the subscriber information.

17. In logs kept in the ordinary course of business, ISPs keep track of the IP addresses assigned to their subscribers. Once provided with an IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and other related information of the user/subscriber.

18. Only the ISP to whom a particular IP address has been assigned for use by its subscribers can correlate that IP address to a particular subscriber. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Thus, to correlate a subscriber with an IP address, the ISP also needs to know when the IP address was being used.

19. Maverickeye UG determined that the Doe Defendants identified in Complaint Exhibit A were using the ISPs listed in the exhibit to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

20. It is possible for digital files to be mislabeled or corrupted; therefore, Maverickeye UG (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the Motion Picture themselves.

21. As to Plaintiff's copyrighted Motion Picture, as identified in the Complaint, a member of Maverickeye UG watches a DVD of the original Motion Picture.

22. After Maverickeye UG identified the Doe Defendants and downloaded the motion pictures they were distributing, Maverickeye UG opened the downloaded files, watched them and confirmed that they contained the Motion Picture identified in the Complaint.

23. To identify the IP addresses of those BitTorrent users who were copying and distributing Plaintiff's copyrighted Motion Maverickeye UG's forensic software scans peer-to-peer networks for the presence of infringing transactions.

24. After reviewing the evidence logs, I isolated the transactions and the IP addresses of the users responsible for copying and distributing the Motion Picture.

25. Through each of the transactions, the computers using the IP addresses identified in Complaint Exhibit A transmitted a copy or a part of a copy of a digital media file of the copyrighted Motion Picture identified by the hash value set forth in Complaint Exhibit A. The IP addresses, hash values, dates and times contained in Complaint Exhibit A correctly reflect what is contained in the evidence logs. The subscribers using the IP addresses set forth in

Complaint Exhibit A were all part of a "swarm" of users that were reproducing, distributing, displaying or performing the copyrighted Motion Picture.

26. Moreover, the users were sharing the exact same copy of the Motion Picture. Any digital copy of an audiovisual work may be uniquely identified by a unique, coded, string of characters called a "hash checksum." The hash checksum is a string of alphanumeric characters generated by a mathematical algorithm known as US Secure Hash Algorithm 1 or "SHA-1". By using a hash tag to identify different copies of the Motion Picture, MEU was able to confirm that these users reproduced the very same copy of the Motion Picture.

27. The MEU software analyzed each BitTorrent "piece" distributed by each IP address listed in Complaint Exhibit A and verified that reassembling the pieces using a specialized BitTorrent client results in a fully playable digital motion picture.

28. The software uses a geolocation functionality to determine the location of the IP addresses under investigations. The location of each IP address is set forth in Complaint Exhibit A. IP addresses are distributed to ISPs by public, nonprofit organizations called Regional Internet Registries. These registries assign blocks of IP addresses to ISPs by geographic region. Master tables correlating the IP addresses with local regions are maintained by these organizations in a publicly-available and searchable format. An IP address' geographic location can be further narrowed by cross-referencing this information with secondary sources such as data contributed to commercial database by ISPs.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 31 day of March, 2016.

By: _____
Daniel Macek